

REMARKS

Claims 1-37 are pending in this application, with claims 1, 15, and 25 being independent.

Claim Rejections – 35 U.S.C. § 102(e)

Claims 1-37 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Number 6,662,230 (“Eichstaedt”).

Applicant respectfully traverses this rejection.

Applicant specifically asks the Examiner to review the following issues:

1. Eichstaedt fails to support the presently pending rejection of claims 1-37 under 35 U.S.C. § 102(e) as it fails to describe or suggest all features and limitations of independent claims 1, 15, and 25. In particular, Eichstaedt fails to describe or suggest “monitoring for connection transactions between multiple access requestors and multiple access providers using a switching component connected to the multiple access providers,” as recited in claim 1 and similarly recited in claims 15 and 25.
2. The arguments presented in the Final Office Action against Applicant’s prior remarks illustrate misinterpretations of Applicant’s prior remarks.

Discussion of Issues:

1. Eichstaedt fails to support the presently pending rejection of claims 1-37 under 35 U.S.C. § 102(e) as it fails to describe or suggest all features and limitations of independent claims 1, 15, and 25. In particular, Eichstaedt fails to describe or suggest “monitoring for connection transactions between multiple access requestors and multiple access providers using a switching component connected to the multiple access providers,” as recited in claim 1 and similarly recited in claims 15 and 25.

Claim 1 recites a method for securing an accessible computer system that includes monitoring for connection transactions between multiple access requestors and multiple access providers using a switching component connected to the multiple access providers, and denying access by an attacking access requestor to the multiple access providers when a number of connection transactions initiated by the attacking access requestor through the switching component exceeds a configurable threshold number during a first configurable period of time.

To illustrate and provide context for the subject matter of claim 1, a non-limiting example described in the specification notes:

Counting component 420 [which is part of switch 170] is capable of counting the number of connection transactions initiated from an access requestor 110 at a single IP address, irrespective of the access provider 190 with which the access requestor 110 seeks to establish a connection. For example, during a first connection transaction, the access requestor 110 from a single IP address may initiate a connection with a first access provider 190, while during a subsequent connection transaction, the access requestor 110 from the same IP address may initiate a connection with a different access provider 190. Counting component 420 may be configured to count and log each of these connection transactions in association with the IP address. Application at page 8, lines 22-30.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 1 because Eichstaedt fails to describe or suggest at least “monitoring for connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers” (emphasis added), as recited in claim 1.

In contrast, Eichstaedt describes a data protection system 11 that monitors for connection transactions between multiple access requestors (e.g., client computers 12 and 14) and a single access provider (e.g., web server 18).¹ In particular, the Eichstaedt's data protection system monitors for connection transactions between the client computers 12 and 14 and the web server

¹ Applicant does not concede that Eichstaedt “monitors for connection transactions;” however, for sake of simplicity of comparing the technology taught by Eichstaedt with the subject matter of claim 1, Applicant assumes that Eichstaedt monitors for connection transactions, as recited in claim 1.

18 for limiting the access by the client computers 12 and 14 to data objects accessed through the web server 18. Col. 6, lines 20-22. To do so, the data protection system 11 intercepts requests from the client computers 12 and 14 to the web server 18 and analyzes the requests. Col. 5, lines 25-30. If the requests meet certain criteria, they are forwarded by data protection system 11 to web server 18, which accesses the database 20 when formulating a response to the requests. Col. 6, lines 35-37. Apparently, the technology described by Eichstaedt protects a single web server, web server 18, from abusive clients seeking to make requests too frequently, or seeking to otherwise absorb too much of the web server's 18 resources. Col. 3, lines 45-49. However, Eichstaedt does not describe or suggest "monitoring for connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1.

Notably, the Final Office Action contends that web server 18 and database 20 of Eichstaedt are both access providers, and therefore concludes that Eichstaedt teaches multiple access providers. Final Office Action at page 3, lines 18-20. Assuming, *arguendo*, that the database 20 also is an access provider, this still fails to describe or suggest "monitoring for connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1. Applicant respectfully asserts that, to monitor for connection transactions between the client computers 12 and 14 and the web server 18 and database 20, there must first be connection transactions between the client computers 12 and 14 and each access provider (e.g., web server 18 and database 20). Stated differently, if the client computers' 12 and 14 requests are only directed to the web server 18 or database 20 and not to both of them, there can not be "monitoring for connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1.

In Eichstaedt, the client computers' 12 and 14 requests are directed only to the web server 18 and not to the database 20. In fact, Eichstaedt does not suggest any awareness by the client computers 12 and 14 of the database 20, much less that the client computers 12 and 14 are directing requests to the database 20. All the client computers' 12 and 14 requests are directed to the web server 18, and as such, the only requests monitored and affected by the data protection system 11 are those directed toward the web server 18. Therefore, Eichstaedt's data protection

system 11 monitors for connection transactions between multiple access requestors (e.g., client computers 12 and 14) and a single access provider (e.g., web server 18).

The impact of differences between the technology described by Eichstaedt and the subject matter of claim 1 is perhaps best illustrated by an example. If a particular client computer 12 is making too many requests (above the set threshold) to the web server 18, then the data protection system 11 will recognize that the client computer's 12 requests passes the set threshold, and the data protection system 11 will refuse the client computer 12 access to the web server 18. Now assume that the client computer 12 makes many requests (but less than a threshold) to the web server 18 and that the client computer 12 concurrently makes many requests (but less than the threshold) to another web server. The data protection system 11 will recognize (1) that the client computer's 12 requests to the web server 18 does not exceed the set threshold, and (2) that the client computer's 12 requests to the other web server also do not exceed the set threshold. The data protection system 11 therefore will allow the client computer 12 to access the web server 18, even if the total aggregated number of the client computer's 12 requests to the web server 18 and the other web server may exceed the set threshold. That is, the data protection system 11 makes the decision for the web server 18 without regard for the client computer 12 interactions with the other web server.

By contrast, the subject matter of claim 1 takes into account the interactions of the client computer 12 with the other web server. And, if the total number of the client computer's 12 requests passes the set threshold, irrespective of which server the requests are directed, the client computer 12 will be denied access to both web servers.

Accordingly, Eichstaedt fails to describe or suggest "monitoring for connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1.

For at least these reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 1 along with its dependent claims.

Similarly, claims 15 and 25 recite features similar to the above recited features of claim 1. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 15 and 25, along with their dependent claims, for at least the reasons presented above with respect to claims 1.

2. The arguments presented in the Final Office Action against Applicant's prior remarks illustrate misinterpretations of Applicant's prior remarks.

In response to Applicant's prior remarks, explaining the shortcomings of Eichstaedt, the Final Office Action asserts "a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim." Final Office Action at page 2, lines 13-15. Applicant believes that this statement resulted from a misunderstanding of Applicant's previous remarks, apologizes for the confusion, and provides the following two clarifying comments with hopes of resolving any ambiguity.

First, in the Applicant's prior remarks, Applicant did not attempt to argue intended use of the claimed subject matter. Rather, Applicant was attempting to point out that Eichstaedt fails to describe or suggest an express limitation required by claim 1. Specifically, Applicant pointed out that Eichstaedt fails to describe or suggest "monitoring for connection transactions between multiple access requestors and multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1.

Second, the structure of Eichstaedt's system fails to perform the function achieved by the subject matter of claim 1. Specifically, even assuming, *arguendo*, that the structure of Eichstaedt's system monitors for connection transactions, it only monitors for connection transactions between an access requestor and a single server. Nowhere does Eichstaedt describe or suggest that its system can be modified to monitor for "connection transactions... [with] multiple access providers using a switching component connected to the multiple access providers" (emphasis added), as recited in claim 1. Accordingly, Applicant respectfully requests reconsideration and withdrawal of claims 1, 15, and 25, along with their dependent claims.

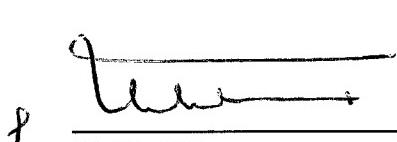
Applicant : Joseph Barrett et al.
Serial No. : 09/666,140
Filed : September 20, 2000
Page : 7 of 7

Attorney's Docket No.: 06975-131001 / Security 08

No fee is believed to be due. However, please apply any other charges or credits to
Deposit Account 06-1050.

Respectfully submitted,

Date: 8/2/2006


(Reg. No. 10250)

W. Karl Renner
Reg. No. 41,265

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331